REMARKS

This amendment is responsive to the Final Office Action[1] having a mailing date of January 12, 2005. Claims 1-6 and 8-22 were presented for examination and have been rejected. All independent claims, namely claims 1, 5, 9, 13, 14 and 22, have been amended herein. Support for these amendments can be found in the application as originally filed. For example, see Fig. 1 and the specification, at least page 5, line 18 through page 6, line 15, discussed further hereinbelow; no new matter is added. No claims are canceled. No claims are added. Thus, claims 1-6 and 8-22 are pending.

Claims 1-6 and 8-22 are rejected under 35 U.S.C. § 102(b) as being anticipated by Sudia et al. (U.S. Patent No. 5,825,880; hereinafter Sudia). The rejection is respectfully traversed because all claim elements of the independent claims are not disclosed or suggested by Sudia, for the following reasons.

Consider amended claim 1:

> In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising: executing an application program at the node which need not be highly secured; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the node; transmitting the message to the cryptographic processing component; and performing the cryptographic-related processing by the cryptographic processing component. (Emphasis added.)

In the Final Office Action, Response to Arguments, page 8, the Examiner takes the position that "the network node" in amended claim 1 in the June 29, 2004 response

[1] The Final Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in , any such statement.

PAGE 11/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729308 * CSID:9727183946 * DURATION (mm-ss):06-12

BEST AVAILABLE COPY

"can broadly be interpreted as any one of the nodes within the network environment." Applicants respectfully disagree. Claim 1, as previously presented in the prior response filed June 29, 2004, was unambiguous regarding which node was being referred-back to. In the preamble of that claim, "a network node" is but one particular node of a network and subsequent recitation of "the network node" can refer back to only the "a network node" previously recited in the preamble and not to any other node in the network.

However, rather than debate this point any further, and solely to facilitate the prosecution of this application, Applicants have amended claim 1 herein in a manner to completely avoid this disagreement. In the above-quoted, and currently-amended, claim 1, "a node" is characterized as being "operative within a network of a plurality of nodes".[2] Accordingly, any subsequent recitation in that claim of "the node", by traditional antecedent claim interpretation, MUST mean the node corresponding to the "a node" and CANNOT mean any other node in the plurality of nodes. Therefore, the method recited in claim 1 is limited to being performed in a single node within the network of a plurality of nodes; i.e., "*In a node* operative within a network of a plurality of nodes, *a method for performing*..." as recited in claim 1 with emphasis added. This is in direct contrast to that operation in Sudia where its methodology, as reflected in its Fig. 2 and described in related portions of its specification, is not performed in a single node (i.e., signing device 39 is securely located *and separated* from message server 47).

However, in addition to the position taken in the Final Office Action as described

[2] This nodal configuration is shown in the instant application, as filed, at least in Fig. 1 and is described in the specification at least on page 5, line 18 through page 6, line 15, thereby providing support for this amendment.

PAGE 12/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID:9727183946 * DURATION (mm-ss):06-12

above, in the Response to Arguments, page 8, the Examiner further alleges that Sudia, in contradiction to its paramount teaching that its signing device and its message server are separated, also teaches that the message server and the signing device *could* be implemented on a single computer, and cites column 7, lines 55-65 in Sudia.

> "As shown, a signing device and its associated message server preferably are divided into two, physically separate computers. Although less preferred, the signing device 39 and message server 47 could be implemented as separate tasks on a single computer *in a highly secure environment*". (Sudia, Column 7, lines 60-65, Emphasis added).

This section discloses that the two physically separate computers are clearly preferred, but *if in a highly secure environment* then the signing device and the message server could be implemented on a single computer. But, by important contrast, Applicants' nodes do not need to be in a highly secure environment. Applicants have thus amended their claims, for example, in currently amended claim 1 above, to include: "*the node which need not be highly secured*" (Emphasis added).

Clearly, Fig. 2 in Sudia in combination with the above-quoted discussion and the discussion in Sudia, column 7, lines 23-25, teach the importance, if not the necessity, of the signing device 39 being placed in a "physically secure location, such as a vault." The above-quoted section says that the signing device and its server are *preferably* divided into separate computers. That separation permits and facilitates the placing of the signing device into a vault. Vaults are discussed and needed in Sudia, possibly because of heightened security requirements imposed by Sudia's "private signature keys" (col. 1, lines 48 - 58; col. 2, lines 4-7; col. 2, lines 53-57; col. 3, lines 21-24, etc.) which are or should be more confidential or sensitive than public keys. But, Applicants' disclosure in

PAGE 13/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID:9727183946 * DURATION (mm-ss):06-12

the instant application is made within the context of a public key infrastructure (title), whereby it does not require the same physically secure standard set forth in Sudia. Applicants' invention is advantageous over Sudia at least for this very reason: "An advantage of the invention is that the applications or network programmer is able to incorporate complex security features without having to gain detailed knowledge of complex *secret* and public key algorithms." (specification, page 13, line 22 through page 14 , line 3, Emphasis added.)

This amendment clearly overcomes any application of Sudia against claim 1. First of all, Sudia plainly prefers its signing device and its associated message server to be divided into two, physically separate computers where Applicants' claim 1 is limited to performing in a single node. Secondly, if they are un-preferably integrated onto a single computer, Sudia teaches that its signing device is placed in a highly secure environment where, by patentable contrast, Applicants' claim 1 recites that its node need not be highly secured.

Applicants' amendment language, "...the node which need not be highly secured" is supported by the application as originally filed. For example, in Applicants' specification, page 6, lines 1-3, it discusses the nodes 110, 120, and 130 of Fig. 1, such nodes along with server 140 and network 150 comprising Applicants' system. As stated therein, those nodes can be any type of computer device. For example, as disclosed therein, those nodes can be "a personal computer, a laptop, a personal digital assistant (PDA) or a similar device with a connection to network 150." Clearly, these examples of nodes from which Applicants' claimed subject matter can be implemented normally are not, and need not be, used in a highly secure environment - e.g., people using a laptop or

PAGE 14/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID:9727183946 * DURATION (mm-ss):06-12

a PDA do not first find their way to a "vault" and then place themselves inside the vault for security purposes before operating their laptop or PDA. Far to the contrary, laptops and PDA's are used in virtually all public spaces such as, for example, airports, airplanes, trains, corporate business environments, etc. Therefore, Applicants' specification as originally filed clearly supports the notion that the "nodes" of its system can be used without a need for their being highly secured, as recited in amended claim 1.

It is respectfully submitted that Sudia does not anticipate claim 1 because it does not disclose or suggest at least: "executing an application program at the node which need not be highly secured" as recited in claim 1, for reasons stated above. MPEP § 2131 states that to anticipate a claim, the reference must teach every element of the claim. Since at least this claim element is not taught by Sudia, it is respectfully requested that the rejection of claim 1 under 35 USC § 102(b) be withdrawn and the claim allowed.

The other independent claims 5, 9, 13, 14 and 22 have been similarly amended, where each independent claim contains a similar limitation relating to its equivalent node (i.e., equivalent to the node which performs the method of Applicants' claim 1) that it need not be highly secured. Therefore, the other independent claims are urged to be likewise allowable for reasons similar to those given above.

It is respectfully submitted that claims 2-4 dependent from claim 1, claims 6 and 8 dependent from claim 5, claims 10-12 dependent from claim 9, and claims 15-21 dependent from claim 14 are also allowable, at least for reasons based on their dependencies from allowable base claims. Furthermore, these dependent claims are independently allowable because they recite additional features not disclosed or

PAGE 15/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID:9727183946 * DURATION (mm-ss):06-12

suggested by Sudia as detailed in the previous response dated June 29, 2004, where those reasons need not be repeated here.

Therefore, in view of the foregoing, it is respectfully submitted that all independent and dependent claims are allowable over the cited reference.

PAGE 16/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID:9727183946 * DURATION (mm-ss):06-12

CONCLUSION

In view of the foregoing amendments and remarks, the Applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application. This amendment after final rejection should be entered by the Examiner because it does not raise new issues, does not require the Examiner to do further searching, and narrows-down the issues that may be presented on appeal should the Examiner not find this amendment sufficiently persuasive to allow all pending claims.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: _____
Joel Wall
Reg. No. 25,648

Date: March 11, 2005
Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code HQE03H14
Irving, Texas 75038
(972) 718-4800
CUSTOMER NO. 32127

PAGE 17/17 * RCVD AT 3/11/2005 5:10:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:8729306 * CSID:9727183946 * DURATION (mm-ss):06-12

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.